What is Claimed is:

1. A method for controlling communications in an identity-based encryption (IBE) system in which a message encrypted using an IBE public key of a recipient is to be sent over a communications network from a sender to the recipient, wherein the recipient is in a district associated with an IBE private key generator from which the recipient obtains an IBE private key for decrypting the message encrypted with the IBE public key, comprising:

at the IBE private key generator, providing district policy information to the sender over the communications network; and

at the sender, using the district policy information in sending the message to the recipient.

2. The method defined in claim 1 wherein using the district policy information at the sender comprises using the district policy information to determine whether to send the message to the recipient.

3. The method defined in claim 1 wherein using the district policy information at the sender comprises using the district policy information and client policy information to determine whether to send the message to the recipient.

4. The method defined in claim 1 wherein using the district policy information at the sender comprises using the district policy information to determine how to send the message to the recipient.

5. The method defined in claim 1 wherein the district policy information includes IBE encryption protocol information, the method comprising using the IBE encryption protocol information at the sender to determine which IBE encryption protocols are being used by the district.

6. The method defined in claim 1 wherein the district policy information includes IBE public key format information, the method comprising using the IBE public key format information from the district policy information at the sender to determine how to construct the IBE public key.

7. The method defined in claim 1 wherein the recipient has a username and wherein the district policy information includes IBE public key format information that specifies which portion of the recipient's username is used to form the IBE public key, the method comprising using the IBE public key format information from the district policy information at the sender to construct the IBE public key from the recipient's username.

8. The method defined in claim 1 wherein the district policy information includes communications protocol information that specifies which communications protocols are used by the district, the method comprising using the communications protocol information at the sender to determine which communications

protocols are being used by the district.

9. The method defined in claim 1 wherein the district policy information includes communications protocol information that specifies which communications protocols are used by the district, the method comprising using the communications protocol information at the sender to determine which message format is being used by the district.

10. The method defined in claim 1 wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district, the method comprising using the authentication protocol information at the sender in sending the message to the recipient.

11. The method defined in claim 1 wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district, the method comprising using the authentication protocol information at the sender to determine whether to send the message to the recipient.

12. The method defined in claim 1 wherein the district policy information includes authentication protocol information that specifies what type of

authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district, the method comprising using the authentication protocol information at the sender to determine whether the recipient uses a smart card when being authenticated by the IBE private key generator.

13. The method defined in claim 1 wherein the district policy information includes content-based protocol information that specifies how messages are to be handled based on their content, the method comprising using the content-based protocol information at the sender to determine whether to send the message to the recipient.

14. The method defined in claim 1 wherein the district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with at least one of the subdistricts, and wherein each subdistrict has associated subdistrict policy information, the method further comprising:

at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and

at the sender, using the subdistrict policy information for the multiple subdistricts in sending the message to the recipient.

15. The method defined in claim 1 wherein the

district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with more than one of the subdistricts, and wherein each subdistrict has associated subdistrict policy information, the method further comprising:

at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and

at the sender, using the subdistrict policy information for the subdistricts with which the recipient is associated in determining which subdistrict to send the message to.

16. The method defined in claim 1 wherein the district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with more than one of the subdistricts, wherein the subdistricts use different techniques for authenticating recipients, wherein each subdistrict has associated subdistrict policy information that specifies the techniques used for authenticating their recipients, the method further comprising:

at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and

at the sender, using the subdistrict policy information for those subdistricts with which the

recipient is associated in determining which of those subdistricts to send the message to based on which technique is used to authenticate the recipient at each of those subdistricts.

17. The method defined in claim 1 wherein the message has certain message content and wherein using the district policy information comprises, at the sender, determining whether to send the message to the recipient based on the message content and the district policy information.

18. The method defined in claim 1 wherein using the district policy information comprises:

at the sender, using the district policy information to determine whether to display a notice for the sender.

19. The method defined in claim 1 wherein providing the district policy information to the sender comprises providing the district policy information in the form of a district policy information list containing an identifier for each list entry.

20. The method defined in claim 1 wherein providing the district policy information to the sender comprises providing the district policy information in the form of a district policy information list having list entries, wherein at least some of the list entries are digitally signed.

21. A method for controlling communications in an identity-based encryption (IBE) system in which a message encrypted using an IBE public key of a recipient is to be sent over a communications network from a sender to the recipient, wherein the recipient is in a district associated with an IBE private key generator from which the recipient obtains an IBE private key for decrypting the message encrypted with the IBE public key, comprising:

at the sender, receiving district policy information for the district; and

at the sender, using the district policy information to determine whether to send the message to the recipient in the district.

22. The method defined in claim 21 wherein using the district policy information at the sender to determine whether to send the message to the recipient in the district comprises using the district policy information and client policy information to determine whether to send the message to the recipient.

23. The method defined in claim 21 wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district and wherein using the district policy information to determine whether to send the message to the recipient in the district comprises using the authentication protocol information at the

sender to determine whether to send the message to the recipient.

24. The method defined in claim 21, further comprising:

at the sender, using identity information associated with the recipient to generate a service name; and

using the service name to obtain the district policy information from a host associated with that service name over the communications network.

25. A method for controlling communications in an identity-based encryption (IBE) system in which a message encrypted using an IBE public key of a recipient is to be sent over a communications network from a sender to the recipient, wherein the recipient is in a district associated with an IBE private key generator from which the recipient obtains an IBE private key for decrypting the message encrypted with the IBE public key, comprising:

at the sender, receiving district policy information for the district; and

at the sender, using the district policy information to determine how to send the message to the recipient in the district.

26. The method defined in claim 25 wherein the district policy information includes IBE encryption protocol information and wherein using the district policy information to determine how to send the message

to the recipient comprises using the IBE encryption protocol information at the sender to determine which IBE encryption protocols are being used by the district.

27. The method defined in claim 25 wherein the district policy information includes IBE public key format information and wherein using the district policy information to determine how to send the message to the recipient comprises using the IBE public key format information from the district policy information at the sender to determine how to construct the IBE public key.

28. The method defined in claim 25, further comprising:

at the sender, using identity information associated with the recipient to generate a service name; and

using the service name to obtain the district policy information from a host associated with that service name over the communications network.